TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

October 2024

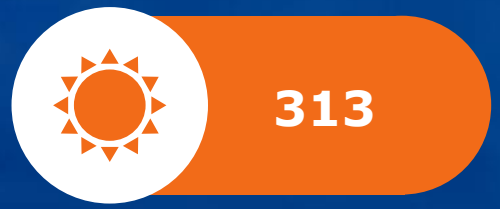
#cyberweather

Cyber weather gives you an update on the key information security incidents and phenomena of the month.

The product is primarily targeted at those who work with information security issues at different levels of organisations. Cyber weather gives readers a quick overview of recent and upcoming events in the field of cyber security.

Cyber weather can be:  calm  worrying  serious

Monthly numbers



The Finnish Transport and Communications Agency Traficom has granted funding worth approximately EUR 6 million to support the development of information security. Funding was granted to 313 companies that are vital to the Finnish society. The sums granted range from EUR 371 to EUR 100,000.

By the end of October, the NCSC-FI has become aware of 16 ransomware cases in Finland this year. The corresponding figure in October 2023 was 25. On average, the NCSC-FI receives approximately 40 ransomware reports each year.

Cyber weather, October 2024

Data breaches and leaks

- A vulnerability in FortiManager resulted in data breaches also in Finland.
- M365 accounts were hacked in a reactivated phishing campaign where victims received a password expiry message.
- In October, the NCSC-FI received reports about low & slow breach attempts that lasted for months. The method relies on small volumes of login attempts over a long period of time.

Scams and phishing

- An aggressive SMS phishing campaign was launched at the end of October with messages sent in the name of various organisations. Purported SMS sender names included correct and incorrect forms of the organisations Terveystalo, Traficom, Fortum and Mehiläinen.
- Fraudulent websites used to steal banking details have been taken down in collaborative efforts by the authorities and internet service providers.

Malware and vulnerabilities

- Fortinet has released a patch for a critical FortiManager vulnerability that has been actively exploited.
- It is important to ensure that home devices are secure. Vulnerable network devices can be exploited to carry out denial-of-service attacks, for example.

Automation and IoT

- Lately, household IoT devices with insufficient security features have been exploited in many cyber security attacks and issues.
- NIST has published a report about barriers to IoT adoption.
- The comprehensive report is largely in line with the NCSC-FI's observations.

Network performance

- In October, seven disturbances were observed in communications networks. Apart from one, all were minor.
- The number of denial-of-service (DoS) attacks is still higher than at the beginning of the year but the situation has calmed down since September.

Spying

- APT groups associated with Russia attempt to spy on central government and defence targets in Europe, the United States and Ukraine.
- A Chinese operator hacked the systems of telecommunications operators and wiretap systems in the United States to gain information about the election.

NCSC-FI's tips and recommendations for improving cyber security preparedness:

The NCSC-FI published an article about ensuring the validity of domain names. Domain names are important intangible assets and can compromise information security if they end up in the wrong hands.

Traficom updated its document on national cryptographic protection requirements by adding quantum-safe algorithms to the national criteria. The key encapsulation algorithm ML-KEM and signature algorithms ML-DSA and SLH-DSA standardised by NIST are approved in national use. Traficom recommends that organisations begin using quantum-safe algorithms as soon as possible.

The revised national Cyber Security Strategy was approved at a government plenary session. In the strategy, cyber security is defined as an integral part of comprehensive security, in which functions vital to society are protected in collaboration among the authorities, trade and industry, organisations and citizens.

The NCSC-FI recommends that all individuals should use multiple means of strong electronic identification to avoid relying on a single operator to access services that require electronic identification.

Overview of cyber security in October

- The number of cyber incident reports received by the NCSC-FI increased in October compared to levels earlier in the autumn.
- Autumn weather has included occasional rainy clouds and grey spells because of recent email and SMS phishing and scam campaigns targeting Finnish organisations. M365 campaigns, in particular, have in some cases resulted in data breaches.
  - SMS scams use sender names with correct and incorrect spellings of the names of actual organisations. The NCSC-FI urges organisations that send text messages to protect their SMS sender IDs as soon as possible.
  - In early October, tens of thousands of people in Finland received a warning message from the police informing recipients that they are under a higher risk to be targeted by criminals. The messages were sent on the basis of a database that the police obtained from criminals. The lists included names, telephone numbers and in some instances also the birth dates of people in Finland.
  - The NCSC-FI disseminates information about active scam campaigns in its weekly reviews and Information Security Now! articles, for example.
- DoS attacks continued actively, just as in previous months. The attacks were targeted against the financial sector and various banks, in particular.

TOP 5 cyber threats in the near future (6–24 months)

1.

Serious vulnerabilities are being exploited faster and faster

In addition to installing an update that fixes the vulnerability, it is often necessary to investigate whether the vulnerability has already been exploited before installing.

2.

Ransomware - Significant threat to organisations

Over the past year, several organisations in Finland have fallen victim to ransomware, and their number is also growing globally.

3.

The information security and continuity of supply and service chains are increasingly critical.

To ensure cyber security, organisations need to understand their own supply chains. Most organisations are more or less dependent on outsourced digital services.

Symbols

New

Updated

4.

Organisations should prepare for AI-related challenges.

Organisations should try to identify challenges that artificial intelligence may cause and prepare for them by training their staff, for example.

5.

Importance of protecting telecommunications infrastructure emphasised

It is important to protect telecommunications and information system infrastructure both abroad and at home, both because of incidents and natural phenomena and because of deliberate disturbances caused by outsiders.

Cyber security trends
in the past 12 months